Exfiltrating Data from Linux Workloads: Uncovering the Techniques

Day Johnson

Microsoft Reactor
March 15th 2023

$~: WHOAMI

DAY JOHNSON
Security Engineer, Datadog

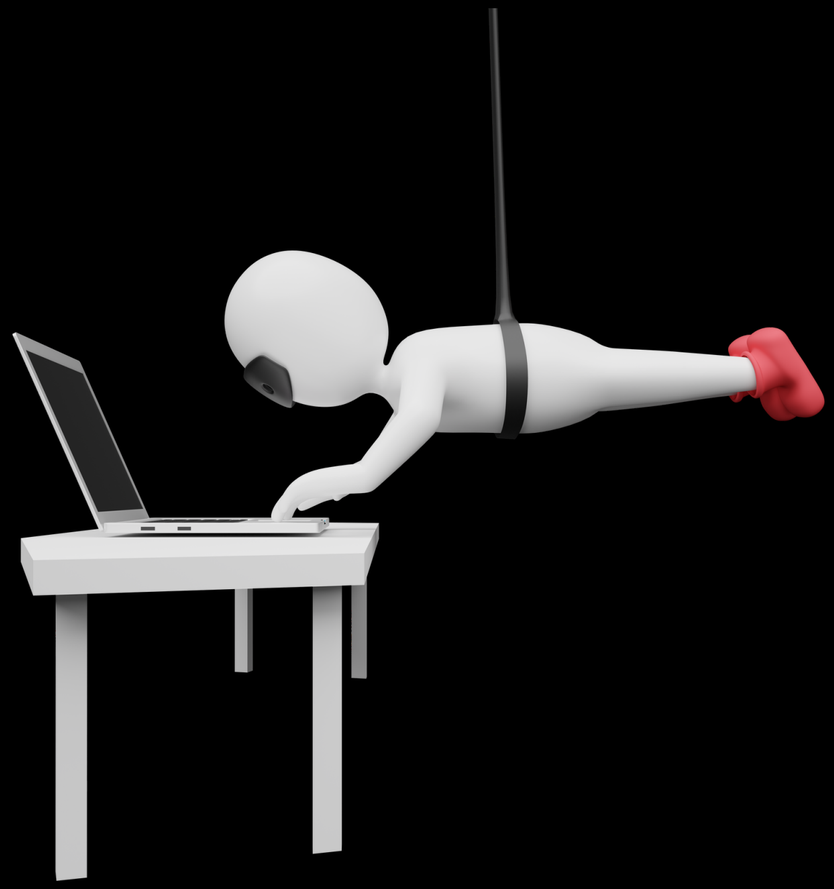
- Security Engineer at Datadog (Cloud Threat Detection)
- Information Technology at WGU
- Cybersecurity Content Creator on YouTube (20k+ Subscribers)
- Founder & Community Manager at Cyberwox Academy
- Cloud Security Content Engineer & Lab Developer
- AWS Community Builder
- Cybersecurity Tutor

@daycyberwox | Day Johnson | daycyberwox.com

AGENDA

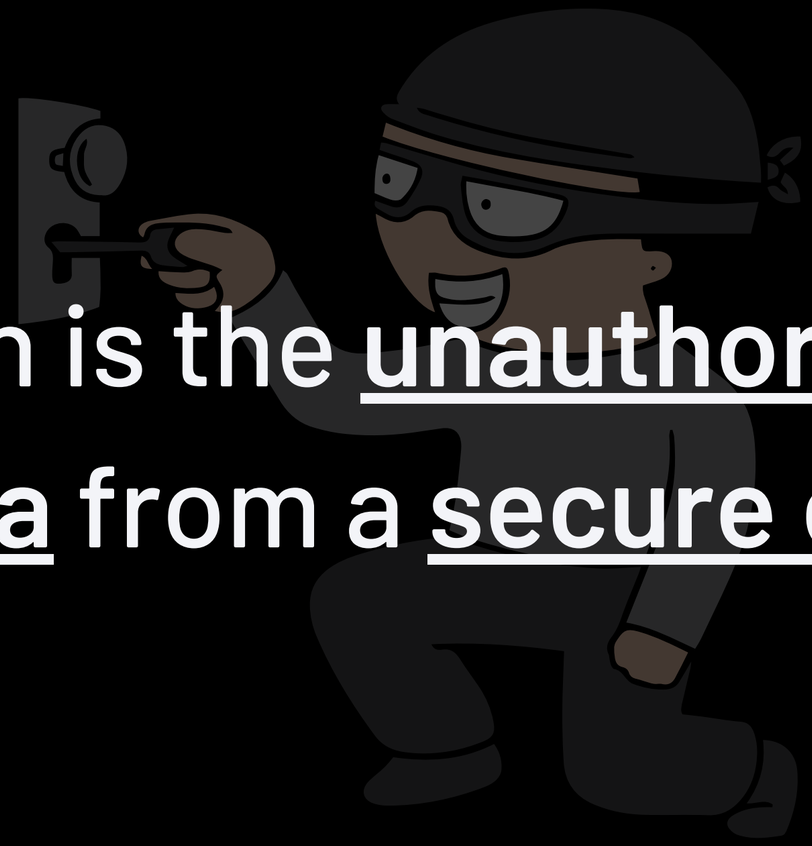
A crash course on how to steal data

1. Data Exfiltration
2. What to steal
3. How to steal
4. Catching a thief
5. Conclusion
6. References



WHAT IS DATA EXFILTRATION

DATA EXFILTRATION



Data exfiltration is the unauthorized transfer of sensitive data from a secure environment.

WHAT TO STEAL?

LINUX WORKLOADS ARE A TREASURE TROVE

BASH COMMAND HISTORY

Bash history contains information about various activities happening on a linux host.

```
→  ~ history | head -10
    1  ifconfig
    2  ping 127.0.0.1
    3  traceroute 127.0.0.1
    4  ssh raspberrypi.local
    5  ssh pi@raspberrypi.local
    6  ssh pi@raspberrypi.local
    7  /Volumes/boot/ssh ; exit;
    8  /Volumes/boot/ssh ; exit;
    9  /Volumes/boot/ssh ; exit;
   10  ls
```

Sytem configurations

Network configurations

~/.bash_history

What commands are being run on this host?

Credentials used for authentication

GIT LOGS

Git logs and configurations contain metadata about commits made in a code repo.

Code vulnerabilities

```
→  learn-to-cloud git:(adding-sec) ✗ clear
commit [redacted]  (HEAD -> adding-sec, origin/adding-sec)
Author: Abisola Dayspring Johnson <dayspring@cumulus.lan>
Date:   Mon Jun 20 23:55:20 2022 -0500

    Fixed minor typos

commit [redacted]
Author: Abisola Dayspring Johnson <dayspring@cumulus.lan>
Date:   Mon Jun 20 23:24:57 2022 -0500

    Added security section

commit [redacted]
Author: Abisola Dayspring Johnson <dayspring@cumulus.lan>
Date:   Mon Jun 20 23:24:05 2022 -0500

    Added security section

commit [redacted]
Author: Gwyneth Pena-Siguenza [redacted]
Date:   Mon Jun 20 21:21:58 2022 -0400

    Added sec phase
```

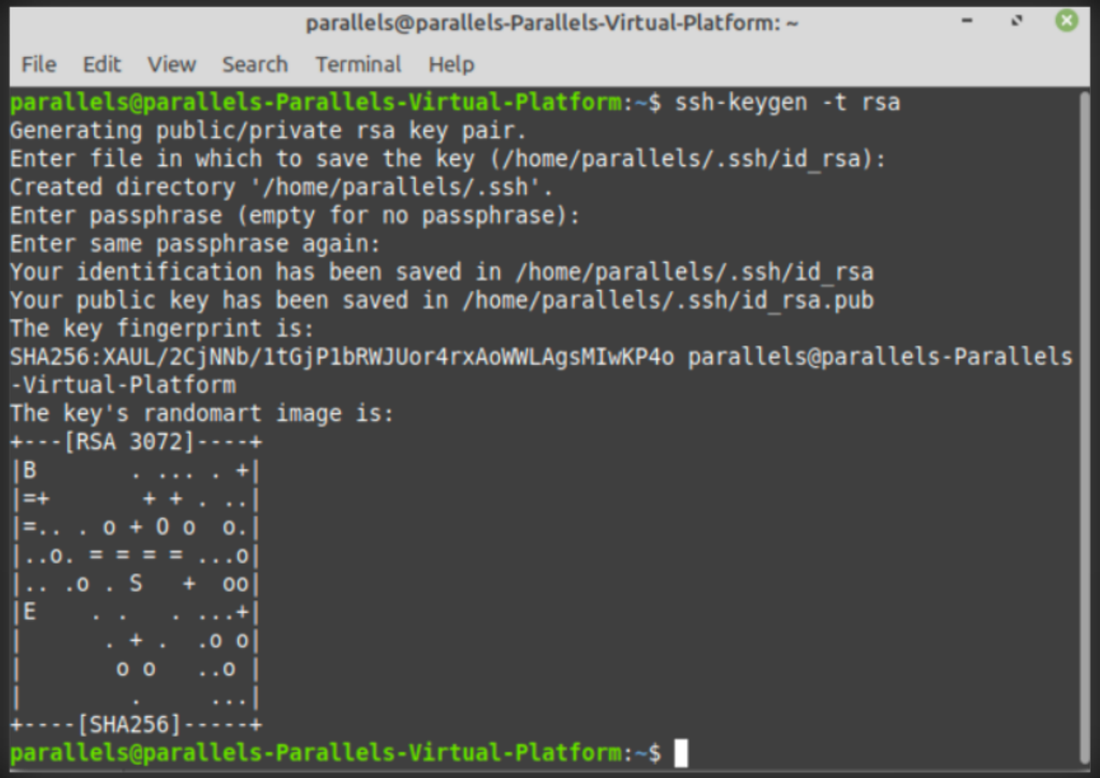
Committed credentials

What commands are being run on this host?

What commits were made?

SSH KEYS

SSH Keys provide secure authentication to a remote host.



Unauthorized access

/.ssh/config

/.ssh/known_hosts

Maintaining persistence

Access hosts within the network

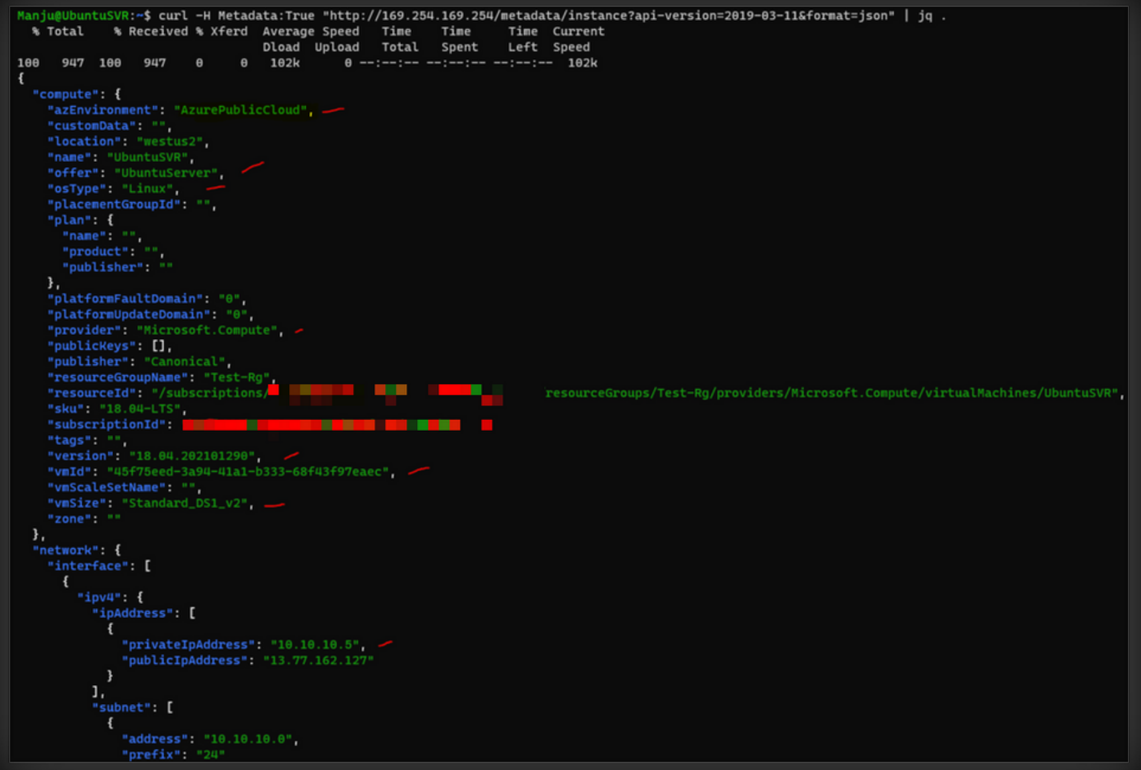
Source: https://jumpcloud.com/blog/what-are-ssh-keys

INSTANCE METADATA

The Azure Instance Metadata Service (IMDS) contains sensitive information about a virtual machine's configuration and metadata.

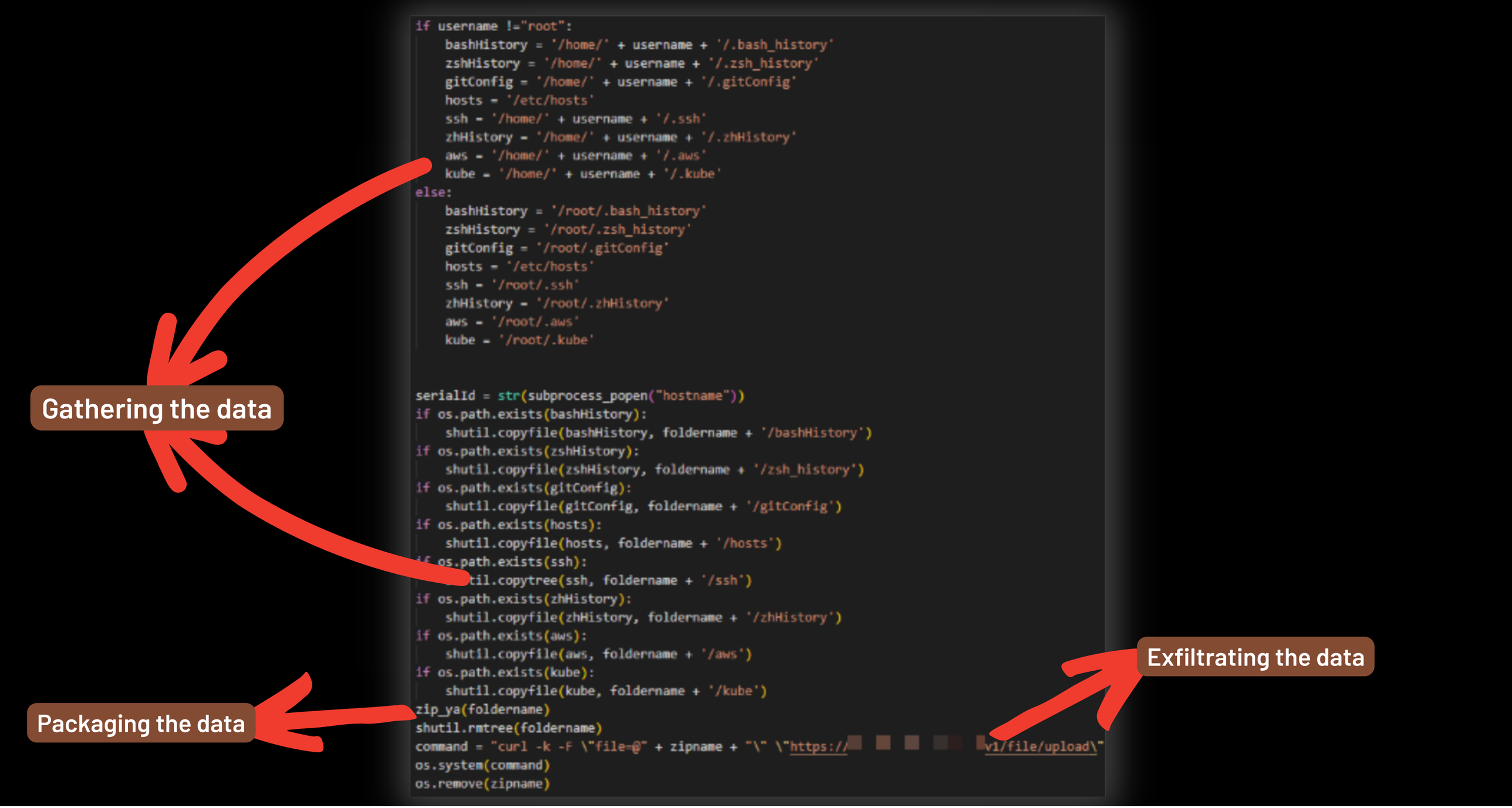
Azure configuration

- *Placement Group*
- *Encryption Keys*
- *Credentials*
- *Admin username*
- *Host Group ID*
- *Password Authentication Config*
- *Resource Group Name*
- *UserData*



Source: https://manjusullad.wordpress.com/2021/02/08/azure-imds2-2/

HOW TO STEAL?

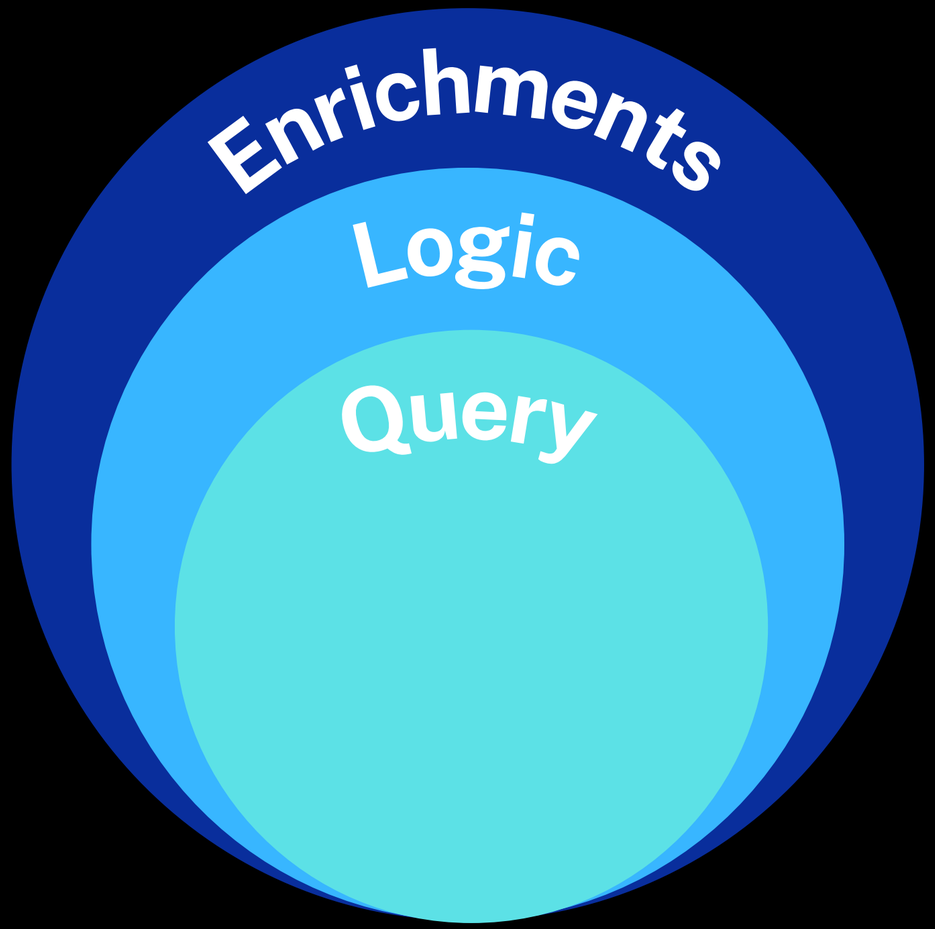


Source: https://www.reversinglabs.com/blog/sentinelsneak-malicious-pypi-module-poses-as-security-sdk

CATCHING A THIEF

DETECTION-AS-CODE

Detection building blocks.



Query

The foundation of your detection. Specific attributes & parameters that define the adversary's activity.

Logic

Defines the methodology of your detection. Here you define rules, thresholds, baselines and logic statements (AND/OR).

Enrichments

Additions like metadata, tagging, exclusions, suppressions, alerting, threat intel and more are considered enrichments.

SIGMA RULE - DATA EXFILTRATION WITH WGET

```yaml
title: Data Exfiltration with Wget
id: cb39d16b-b3b6-4a7a-8222-1cf24b686ffc
status: test
description: |
    Detects attempts to post the file with the usage of wget utility.
    The adversary can bypass the permission restriction with the misconfigured sudo permission for wget utility which could allow them to read files like /etc/shadow.
references:
    - https://linux.die.net/man/1/wget
    - https://gtfobins.github.io/gtfobins/wget/
author: 'Pawel Mazur'
date: 2021/11/18
modified: 2022/12/25
tags:
    - attack.exfiltration
    - attack.t1048.003
logsource:
    product: linux
    service: auditd
detection:
    selection:
        type: EXECVE
        a0: wget
        a1|startswith: '--post-file='
    condition: selection
falsepositives:
    - Legitimate usage of wget utility to post a file
level: medium
```

Source: https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_data_exfil_wget.yml

SIGMA RULE - DATA EXFILTRATION WITH WGET

```yaml
title: Data Exfiltration with Wget
id: cb39d16b-b3b6-4a7a-8222-1cf24b686ffc
status: test
description: |
    Detects attempts to post the file with the usage of wget utility.
    The adversary can bypass the permission restriction with the misconfigured sudo permission for wget utility which could allow them to read files like /etc/shadow.
references:
    - https://linux.die.net/man/1/wget
    - https://gtfobins.github.io/gtfobins/wget/
author: 'Pawel Mazur'
date: 2021/11/18
modified: 2022/12/25
tags:
    - attack.exfiltration
    - attack.t1048.003
logsource:
    product: linux
    service: auditd
detection:
    selection:
        type: EXECVE
        a0: wget
        a1|startswith: '--post-file='
    condition: selection
falsepositives:
    - Legitimate usage of wget utility to post a file
level: medium
```

Source: https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_data_exfil_wget.yml

SIGMA RULE - DATA EXFILTRATION WITH WGET

```yaml
title: Data Exfiltration with Wget
id: cb39d16b-b3b6-4a7a-8222-1cf24b686ffc
status: test
description: |
    Detects attempts to post the file with the usage of wget utility.
    The adversary can bypass the permission restriction with the misconfigured sudo permission for wget utility which could allow them to read files like /etc/shadow.
references:
    - https://linux.die.net/man/1/wget
    - https://gtfobins.github.io/gtfobins/wget/
author: 'Pawel Mazur'
date: 2021/11/18
modified: 2022/12/25
tags:
    - attack.exfiltration
    - attack.t1048.003
logsource:
    product: linux
    service: auditd
detection:
    selection:
        type: EXECVE
        a0: wget
        a1|startswith: '--post-file='
    condition: selection
falsepositives:
    - Legitimate usage of wget utility to post a file
level: medium
```

ENRICHMENTS

Source: https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_data_exfil_wget.yml

EXFILTRATION ATTEMPT WITH CURL

Things to look out for:

-k or -insecure allows data transfer over insecure & unencrypted connections

-s or --silent performs data transfer in "silent" or "quiet mode”

-F or --form for filling in web forms during POST request

-T or --upload-file or file uploads over FTP

-X or --request for specifying a custom request method such as POST

BRINGING IT ALL TOGETHER

- Linux hosts are a treasure trove of data
- Bash history, Git logs, SSH Keys & IMDS are attractive to attackers
- WGET & CURL are common utilities used for exfiltration
- Detection-as-code helps in catching attackers

SOURCES & REFERENCES

https://attack.mitre.org/techniques/T1552/003/
https://blog.aquasec.com/threat-alert-kinsing-malware-container-vulnerability
https://www.c4isrnet.com/opinion/2017/08/31/cybersecurity-from-the-infrastructure-up-dont-ignore-ssh-keys-commentary/
https://jumpcloud.com/blog/what-are-ssh-keys
https://manjusullad.wordpress.com/2021/02/08/azure-imds2-2/
https://medium.com/marcus-tee-anytime/steal-secrets-with-azure-instance-metadata-service-dont-oversight-role-based-access-control-a1dfc47cffac
https://learn.microsoft.com/en-us/azure/virtual-machines/instance-metadata-service?tabs=linux
https://learn.microsoft.com/en-us/azure-stack/user/instance-metadata-service?view=azs-2206
https://www.reversinglabs.com/blog/sentinelsneak-malicious-pypi-module-poses-as-security-sdk
https://github.com/SigmaHQ/sigma/blob/master/rules/linux/auditd/lnx_auditd_data_exfil_wget.yml
https://medium.com/maverislabs/bash-tricks-for-file-exfiltration-over-http-s-using-flask-112aed524ad
https://documentation.observeit.com/insider_threat_library/data_exfiltration.htm